

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN MARIANA ISLANDS

MC 21 00005

IN THE MATTER OF THE SEARCH OF:

Miscellaneous Case No.

A&A ENTERPRISES CNMI, LLC office
building located on Espana Street, off of
Middle Road in Gualo Rai, Saipan

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH
WARRANT**

I, Frederic Jonas, being first duly sworn, do hereby state as follows:

I. INTRODUCTION

1. I am a Special Agent (SA) with U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed since July, 2019, and have been assigned to the HSI Saipan office in the Commonwealth of the Northern Mariana Islands (CNMI) since February, 2020. My training includes completion of the Criminal Investigator Training Program and ICE Special Agent Training Program which I received at the Federal Law Enforcement Training Center (FLETC) in Glynnco, Georgia. I have also received extensive classroom and on-the-job training in the areas of general law enforcement, criminal investigative techniques, and criminal law including search and seizure.

2. My duties as an HSI Special Agent include investigating criminal and administrative violations of Federal laws outlined in Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I have led or directly participated in criminal investigations including (but

not limited to) investigations of visa and immigration document fraud-related offenses. Investigative techniques that I have relied upon in the course of conducting my investigations include victim, witness, and suspect interviews, review of documents and records (in paper or digital format) obtained through database checks, subpoena, court order, or consent, and physical and electronic surveillance. I am the case agent in an HSI Saipan investigation into a business operating on Saipan called A & A ENTERPRISES CNMI, LLC. (hereinafter A&A ENTERPRISES).

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of the premises further described in Attachment A and the paragraphs below, namely the offices of A&A ENTERPRISES and Alejandro Tumando NARIO, (hereinafter "NARIO") an officer of the business, [REDACTED] an officer of the business, [REDACTED] (hereinafter "[REDACTED]") an employee of the business, and Mylene CASUPANAN, (hereinafter "CASUPANAN") an employee of the business. This office is located off Middle Road on Espana Street in Gualo Rai village, Saipan, MP, and is described as a green colored, one-story concrete structure believed to contain one interior room or work area and an enclosed single bathroom. The public entrance to the office is on the southern face of the building, and the building exterior has distinct white, green, and black lettering that reads "A & A ENTERPRISE, CONSTRUCTION, MANPOWER SERVICES AND GROUND MAINTENANCE". I request this warrant to search the aforementioned premises and seize any evidence of violations of Title 18 U.S. Code § 1546, Fraud and Misuse of Visas, Title 18 U.S.C. § 1341, Mail Fraud, and Title 18 U.S.C. § 371, Conspiracy to Defraud the United States. Evidence to be searched for and seized during the search is more particularly described in the following paragraphs and in

Attachment B. Title 18 U.S.C. § 1546(a) makes it a Federal crime to knowingly make a materially false statement to a U.S. immigration agency under oath or penalty of perjury on an application required by immigration laws or regulations. According to Ninth Circuit Model Jury Instruction No. 8.134, the pertinent elements of a violation of Title 18 U.S.C. § 1546(a) are as follows:

- a. First, the defendant made, or subscribed as true, a false statement;
- b. Second, the defendant acted with knowledge that the statement was untrue;
- c. Third, the statement was material to the activities or decisions of the U.S. Citizenship and Immigration Services (USCIS) agency, in that it had a natural tendency to influence, or was capable of influencing, USCIS's decisions or activities;
- d. Fourth, the statement was made under oath or penalty of perjury; and
- e. Fifth, the statement was made on an application, affidavit, or other document required by immigration laws or regulations.

4. According to Ninth Circuit Model Jury Instruction No. 8.121, the pertinent elements of a violation of Title 18 U.S.C. § 1341 are as follows:

- a. First, the defendant knowingly participated in, devised, or intended to devise a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;
- b. Second, the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;
- c. Third, the defendant acted with the intent to defraud; that is, the intent to deceive or cheat; and
- d. Fourth, the defendant used, or caused to be used, the mails to carry out or attempt to carry out an essential part of the scheme.

5. According to the Ninth Circuit Model Jury Instruction No. 8.21, the pertinent elements of a violation of 18 U.S.C. § 371 are as follows:

- a. First, there was an agreement between two or more persons to defraud the United States by obstructing the lawful functions of USCIS by deceitful or dishonest means as charged in the indictment;
- b. Second, the defendant became a member of the conspiracy knowing of at least one of its objects and intending to help accomplish it; and
- c. Third, one of the members of the conspiracy performed at least one overt act for the purpose of carrying out the conspiracy, with all of you agreeing on a particular overt act that you find was committed.

The facts set forth herein are based on my direct involvement in this investigation, on interviews I conducted of individuals identified in the course of this investigation, my conversations with law enforcement officers having direct or hearsay knowledge of pertinent facts, my review of any official documents and records generated and maintained by various local and federal agencies, and information gained through my own training and experience. I have also discussed the facts of this investigation with other law enforcement officials within HSI who have more extensive experience in business and financial criminal investigations than I, and whom shared with me the substance of their experiences in conducting investigations of this nature. All of the statements and information contained in this affidavit are true and correct to the best of my knowledge and belief.

6. Based on my training, experience, and prior discussions with other experienced law enforcement officials within HSI, I am aware that it is generally common practice for businesses to generate and keep records pertaining to clients, vendors, payments, banking and financial transactions, taxes, and employees in their office. These records generally include (but are not limited to) draft and executed contracts, purchase orders, agreements, employee personnel files, invoices, payments made and received, accounts payable and receivable, accounting and payroll ledgers, transaction receipts and duplicates, business checks, and official

1 correspondence to include electronic mail (e-mail). I know that businesses commonly generate
2 or maintain these records in electronic format, using various types of electronic devices including
3 personal desktop computers, laptop computers, personal digital assistants, tablet devices,
4 smartphones, external hard disk drives, memory sticks, and compact discs or DVDs. I am also
5 aware that businesses are able to convert paper records into electronic format through existing
6 software available to the public. Furthermore, these electronic records can be transmitted via the
7 internet using electronic devices such as personal desktop computers, laptop computers, personal
8 digital assistants, tablet devices, and smartphones, provided the device is connected to the
9 internet.

10 7. Because this affidavit is being submitted for the limited purpose of securing a
11 warrant to search the described premises, I have not included each and every fact known to me
12 concerning this investigation. I have set forth only those facts that I believe are necessary to
13 establish probable cause to believe that evidence of violations of Title 18 U.S. Code § 1546, Title
14 18 U.S.C. § 1341, and Title 18 U.S.C. § 371 are located within the aforementioned premises.
15 Facts not set forth or incorporated herein are not being relied upon in reaching my conclusion
16 that a search warrant should be issued.

17 **II. SUMMARY OF INVESTIGATION**

18 8. During 2020, HSI learned of a scheme where A&A ENTERPRISES located in the
19 Commonwealth of Northern Mariana Islands (CNMI) petitioned for CW-1 visas for applicants
20 located in the Republic of the Philippines. These applicants were promised employment in the
21 CNMI and are required to pay a fee for their recruitment, which includes the petition fee for the
22 CW-1 visa. Upon their arrival in the CNMI, these foreign nationals were told that there was no
23 work for them and/or instructed to find employment elsewhere. A number of these non-working
24

1 employees were instructed to pay employment taxes even though they are not receiving any
2 wages thus falsely representing a full-time employer-employee relationship. HSI has conducted
3 several interviews with foreign nationals that have provided information on the scheme.
4 Furthermore, a database search of CW-1 petitions for A&A ENTERPRISES revealed that
5 numerous petitions were submitted to USCIS for adjudication, for approximately 198 CW-1
6 workers in FY 2019 and FY 2020.

7 **III. PROBABLE CAUSE**

8 9. During the course of this investigation, I and other HSI law enforcement officials
9 have reviewed numerous CW-1 visa application packets submitted by A&A ENTERPRISES to
10 USCIS. Most of the A & A ENTERPRISES petitions were signed by NARIO. The visa packets
11 submitted by A&A ENTERPRISES included numerous documents and records in support of
12 CW-1 visas for prospective employees of A&A ENTERPRISES. Many of these prospective
13 employees are citizens and nationals of the Republic of the Philippines, People's Republic of
14 Bangladesh, and the People's Republic of China.

15 10. These CW-1 visa packets included I-129 CW Petitions for CNMI-Only
16 Nonimmigrant Transitional Worker application forms, copies of service agreements or contracts
17 between A&A ENTERPRISES and several business entities in Saipan, copies of identification
18 documents, clearances, and employment contracts between A&A ENTERPRISES and the
19 employees being petitioned. These packets also included copies of correspondence between
20 USCIS and A&A ENTERPRISES, copies of tax documents and bank account statements for
21 A&A ENTERPRISES, copies of non-discrimination and worker's compensation policies, and
22 public announcement of positions in CNMI newspapers.

23 11. On September 29, 2020, I interviewed Individual 1, a citizen of the Republic of
24 the Philippines, at the HSI Saipan office. Individual 1 stated that while he/she resided in the

1 Philippines he/she became aware of A&A ENTERPRISES from a friend residing in Saipan.
2 Individual 1 stated that his/her friend paid CASUPANAN, an employee of A&A
3 ENTERPRISES, \$660.00 United States Dollars (USD) for Individual 1's CW-1 petition. In
4 addition, Individual 1 obtained a loan for 56,000.00 Php (Philippine Peso), approximately
5 \$1,155.77 USD, in the Philippines to pay for a portion of the CW-1 fees he/she was charged.

6 12. After receiving an approved CW-1 visa, Individual 1 travelled to the United
7 States on February 22, 2020, and was admitted at the Guam International Airport and later
8 travelled to Saipan. Since arriving in Saipan, Individual 1 stated that he/she has never worked
9 for A&A ENTERPRISES and was told there was no work available because of the COVID
10 lockdown. A&A ENTERPRISES told Individual 1 that they would contact him/her when work
11 would become available.

12 13. On or about March 4, 2020, Individual 1 went to A&A ENTERPRISES and paid
13 four hundred \$400 USD to [REDACTED] the secretary at A&A ENTERPRISES, for the renewal of
14 his/her CW-1 visa. Individual 1 also signed an A&A ENTERPRISES employment contract,
15 which was similar to the contract he/she previously signed in the Philippines.

16 14. Individual 1 stated that when he/she makes payments, usually [REDACTED] collects the
17 money at A&A ENTERPRISES' office. [REDACTED] creates a receipt every time Individual 1 makes
18 an employment fee payment, from the same receipt book, and gives a copy of the receipt to
19 him/her. Individual 1 recalled that [REDACTED] normally keeps the receipt book on the top of [REDACTED]
20 desk. The last time Individual 1 received a receipt from A&A ENTERPRISES was on June 15,
21 2020.

22 15. Individual 1 provided your affiant with seven (7) A&A ENTERPRISES receipts
23 for a total of \$3,089.26 USD made at various times from November 12, 2019, to June 15, 2020,
24

1 for the CW-1 processing fee and payments. It was noted that all receipts were handwritten on a
2 serialized custom receipt believed to have originated from a tear-off receipt book.

3 16. On September 29, 2020, I interviewed Individual 2, a citizen of the Republic of
4 the Philippines, at the HSI office. Individual 2 stated that on February 22, 2020, he/she arrived
5 at Guam and subsequently travelled to Saipan. Individual 2 was admitted to the United States
6 utilizing a CW-1 visa, which was petitioned by A&A ENTERPRISES. Since arriving in Saipan,
7 Individual 2 was told by A&A ENTERPRISES that they would contact him/her when work
8 would be available.

9 17. During March 2020, Individual 2 worked at a gas station for sixteen (16) hours at
10 a rate of seven dollars and thirty-five (\$7.35) per hour. This job was arranged by A&A
11 ENTERPRISES and he/she was paid in cash by CASUPANAN. Aside from this brief
12 employment, Individual 2 has not been provided with regular work from A&A ENTERPRISES.

13 18. According to Individual 2, he/she borrowed money from a relative to pay \$2,000
14 USD to A&A ENTERPRISES for the CW-1 visa. Individual 2 stated that his/her relative
15 resided in Saipan and paid \$2,000 USD to A&A ENTERPRISES.

16 19. According to Individual 2, CASUPANAN told him/her that he/she must pay taxes
17 for the seventy (70) hours of "work" at A&A ENTERPRISES and if he/she doesn't, they would
18 cancel his/her CW-1 visa. Therefore, Individual 2 pays CASUPANAN at A&A ENTERPRISES
19 \$194 USD every two (2) weeks for taxes, even though he/she is not earning any wages.
20 Individual 2 stated that CASUPANAN provides him/her with a receipt for each payment.

21 20. Individual 2 stated that [REDACTED] is CASUPANAN's assistant at A&A
22 ENTERPRISES and NARIO is the owner of A&A ENTERPRISES, which is located in Gualo
23
24

1 Rai village on the Island of Saipan. Based on his/her interactions with [REDACTED] and NARIO,
2 Individual 2 believes that they are aware of the taxes that he/she is paying to CASUPANAN.

3 21. During the interview, Individual 2 provided two (2) A&A ENTERPRISES
4 receipts for a total of \$1,074.16 USD. The two receipts were dated June 1, 2020, and June 15,
5 2020, for CW-1 processing fee payments. Both receipts were handwritten on a serialized custom
6 receipt and is believed to have originated from a tear-off receipt book.

7 22. Additionally, Individual 2 provided your affiant with twelve (12) A&A
8 ENTERPRISES service receipts that appear to have been generated and printed on a computer
9 using word processing software, with receipt numbers, date, customer name, job description,
10 name of worker, pay period, hours, rate earned, and total amount for the months of June 2020
11 and September 2020.

12 23. On October 22, 2020, at the direction of HSI, Individual 1 and Individual 2 met
13 with the staff at A&A ENTERPRISES for the purpose of obtaining information about the "taxes"
14 being paid to A&A ENTERPRISES. Individual 1 and Individual 2's conversation was
15 monitored and recorded during this meeting at A&A ENTERPRISES' office. At the conclusion
16 of the meeting, Individual 1 and Individual 2 were separately interviewed by HSI personnel.

17 24. According to Individual 1, NARIO and CASUPANAN were present in the office
18 when he/she asked about the consultation letter he/she received from A&A ENTERPRISES.
19 NARIO told Individual 1 that he/she has not been paying the employment fee. NARIO told
20 Individual 1 that if he/she does not pay the employment fee, i.e. taxes, then they will cancel
21 his/her CW-1 visa. However, if Individual 1 continues to pay his/her employment fee, A&A
22 ENTERPRISES will not cancel his/her CW-1 visa.

23 25. CASUPANAN told Individual 1 that the employment fee was \$194 USD and
24

1 must be paid every two (2) weeks. CASUPANAN explained that the employment fee of \$194
2 USD is the payment for the taxes, rental, and the salary of the employees at A&A
3 ENTERPRISES. NARIO and CASUPANAN explained to Individual 1 it was not their
4 responsibility to find him/her work because it was his/her friend and Individual 2's relative that
5 asked A&A ENTERPRISES for help with obtaining CW-1 visas for them. Therefore, they
6 petitioned for Individual 1 and Individual 2's CW-1 visas and that A&A ENTERPRISES is not
7 responsible for finding work for them.

8 26. During a separate interview, Individual 2 informed me that NARIO and
9 CASUPANAN were present when they entered A&A ENTERPRISES. Individual 2 stated that
10 CASUPANAN opened the front door and he/she observed computers and file cabinets at A&A
11 ENTERPRISES' office.

12 27. On October 26, 2020, HSI Special Agent (SA) Michael Lansangan reviewed the
13 recordings between Individual 1, Individual 2, NARIO and CASUPANAN. In summary, SA
14 Lansangan noted that it contained discussions referencing past arrangements between Individual
15 2's relative and A&A ENTERPRISES to bring Individual 2 to Saipan. The conversation
16 between Individual 1, Individual 2, NARIO and CASUPANAN refers to an agreement with
17 Individual 1's friend, which Individual 1 is now attempting to change. NARIO told Individual 1
18 the reason A&A ENTERPRISES processed the CW-1 petition was because the friend had
19 requested that A&A ENTERPRISES do it for him/her and they had no reason to hire Individual
20 1 if the friend did not request it. NARIO told Individual 1 because the friend had asked them to
21 bring him/her to Saipan then the friend should find him/her work.

22 28. During their conversation, they told Individual 1 that A&A ENTERPRISES has
23 given Individual 1 and Individual 2 many opportunities to find work since their arrival and that
24

1 A&A ENTERPRISES cannot because they will get caught. NARIO told Individual 1 that he/she
2 is to find his/her own way to earn his/her contribution to the agency, i.e. A&A ENTERPRISES.
3 Furthermore, NARIO told Individual 1 that “it is not just you, there are many others who already
4 entered that are in the same situation, but they fulfill their obligation.” NARIO told them, if
5 Individual 1 and Individual 2 do not have work, A&A ENTERPRISES will cancel their
6 paperwork, i.e. CW-1, because all their employees might be implicated or comprised.

7 29. On February 8, 2021, I reviewed the CW-1 petition that was submitted by A&A
8 ENTERPRISES for Individual 1 and Individual 2, Receipt Number: [REDACTED], which
9 appeared to be signed by NARIO and listed the company’s email as

10 [REDACTED] The petition was approved on December 13, 2019, by USCIS
11 for the period of December 13, 2019, to September 30, 2020, and listed the U.S. Consulate as
12 Manila. The petition contained two (2) employment contracts for Individual 1 and Individual 2
13 to be employed by A&A ENTERPRISES, in the job classification of maid and housekeeping
14 from the period of November 20, 2019, until September 30, 2020, for a total of 35 hours per a
15 week.

16 30. The petition also contained two (2) service contract agreements with A&A
17 ENTERPRISES and Individual 3; A&A ENTERPRISES and Individual 4 to employ Individual 1
18 and Individual 2, respectively. The service contract agreement was for Individual 3 and
19 Individual 4 to employ Individual 1 and Individual 2 from A&A ENTERPRISES in the job
20 classification of maid and housekeeping from period of November 20, 2019 until September 30,
21 2020, for a total of 35 hours per a week. Both service contract agreements were signed by
22 Individual 3, Individual 4 and NARIO.

31. On November 18, 2020, the friend of Individual 1, a citizen of the Republic of the Philippines, was interviewed by your affiant at the HSI office. During the interview, the friend stated that he/she asked CAPSUPANAN for help with obtaining a CW-1 visa for Individual 1. It was agreed that the friend would pay for all expenses and fees, he/she therefore paid about \$2,200 to \$2,300 USD in cash installments for Individual 1's CW-1. The friend was told by CAPSUPANAN to find someone that can pose as a second party employer for Individual 1. The friend stated that Individual 4, his/her friend, might be willing to sign and CAPSUPANAN provided him/her with the service contract.

32. The friend took the service contract to Individual 4. At first Individual 4 did not want to sign the document but agreed after he/she spoke with someone from A&A ENTERPRISES. The friend told Individual 4 that the service contract was only going to be used to file for the CW-1 and that the employee-employer relationship would not be real. After he/she signed the contract, the friend took it to CAPSUPANAN at A&A ENTERPRISES.

33. On December 1, 2020, I interviewed Individual 4, a citizen of the Republic of the Philippines, at the HSI office. During the interview, Individual 4 was presented with a service contract between A&A ENTERPRISES and Individual 4. After reviewing the document, Individual 4 stated the signature was his/hers and that he/she had received this document from the relative, his/her friend, and signed as a favor. Individual 4 stated that he/she has never employed Individual 1 and that he/she does not know NARIO or the company A&A ENTERPRISES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

35. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

36. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

37. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

38. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

1 39. *Forensic evidence.* As further described in Attachment B, this application seeks
2 permission to locate not only electronically stored information that might serve as direct
3 evidence of the crime described on the warrant, but also forensic evidence that establishes how
4 the Device was used, the purpose of its use, who used it, and when. There is probable cause to
5 believe that this forensic electronic evidence might be on any such devices found because:

6 40. Data on the storage medium can provide evidence of a file that was once on the
7 storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a
8 paragraph that has been deleted from a word processing file). Virtual memory paging systems
9 can leave traces of information on the storage medium that show what tasks and processes were
10 recently active. Web browsers, e-mail programs, and chat programs store configuration
11 information on the storage medium that can reveal information such as online nicknames and
12 passwords. Operating systems can record additional information, such as the attachment of
13 peripherals, the attachment of USB flash storage devices or other external storage media, and the
14 times the computer was in use. Computer file systems can record information about the dates
15 files were created and the sequence in which they were created.

16 41. Forensic evidence on a device can also indicate who has used or controlled the
17 device. This “user attribution” evidence is analogous to the search for “indicia of occupancy”
18 while executing a search warrant at a residence.

19 42. A person with appropriate familiarity with how an electronic device works may,
20 after examining this forensic evidence in its proper context, be able to draw conclusions about
21 how electronic devices were used, the purpose of their use, who used them, and when.

22 43. The process of identifying the exact electronically stored information on a storage
23 medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic
24

1 evidence is not always data that can be merely reviewed by a review team and passed along to
2 investigators. Whether data stored on a computer is evidence may depend on other information
3 stored on the computer and the application of knowledge about how a computer behaves.
4 Therefore, contextual information necessary to understand other evidence also falls within the
5 scope of the warrant.

6 44. *Nature of examination.* Based on the foregoing, and consistent with Rule
7 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent
8 with the warrant. The examination may require authorities to employ techniques, including but
9 not limited to computer-assisted scans of the entire medium, that might expose many parts of the
10 device to human inspection in order to determine whether it is evidence described by the warrant.

11 45. *Necessity of seizing or copying entire computers or storage media.* In most cases,
12 a thorough search of a premises for information that might be stored on storage media often
13 requires the seizure of the physical storage media and later off-site review consistent with the
14 warrant. In lieu of removing storage media from the premises, it is sometimes possible to make
15 an image copy of storage media. Generally speaking, imaging is the taking of a complete
16 electronic picture of the computer's data, including all hidden sectors and deleted files. Either
17 seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded
18 on the storage media, and to prevent the loss of the data either from accidental or intentional
19 destruction. This is true because of the following:

20 46. The time required for an examination. As noted above, not all evidence takes the
21 form of documents and files that can be easily viewed on site. Analyzing evidence of how a
22 computer has been used, what it has been used for, and who has used it requires considerable
23 time, and taking that much time on premises could be unreasonable. As explained above,
24

1 because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be
2 necessary to thoroughly examine storage media to obtain evidence. Storage media can store a
3 large volume of information. Reviewing that information for things described in the warrant can
4 take weeks or months, depending on the volume of data stored, and would be impractical and
5 invasive to attempt on-site.

6 47. Technical requirements. Computers can be configured in several different ways,
7 featuring a variety of different operating systems, application software, and configurations.
8 Therefore, searching them sometimes requires tools or knowledge that might not be present on
9 the search site. The vast array of computer hardware and software available makes it difficult to
10 know before a search what tools or knowledge will be required to analyze the system and its data
11 on the Premises. However, taking the storage media off-site and reviewing it in a controlled
12 environment will allow its examination with the proper tools and knowledge.

13 48. Variety of forms of electronic media. Records sought under this warrant could be
14 stored in a variety of storage media formats that may require off-site reviewing with specialized
15 forensic tools.

16 49. *Nature of examination.* Based on the foregoing, and consistent with Rule
17 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying
18 storage media that reasonably appear to contain some or all of the evidence described in the
19 warrant, and would authorize a later review of the media or information consistent with the
20 warrant. The later review may require techniques, including but not limited to computer-assisted
21 scans of the entire medium, that might expose many parts of a hard drive to human inspection in
22 order to determine whether it is evidence described by the warrant.

1 50. A&A ENTERPRISES is a functioning company that may conduct legitimate
2 business beyond the scope of that requested in the search warrant. The seizure of A&A
3 ENTERPRISES' computers may limit its ability to conduct its legitimate business. As with any
4 search warrant, Affiant expects that this warrant will be executed reasonably. Reasonable
5 execution will likely involve conducting an investigation on the scene of what computers, or
6 storage media, must be seized or copied, and what computers or storage media need not be
7 seized or copied. Where appropriate, officers will copy data, rather than physically seize
8 computers, to reduce the extent of disruption. If employees of A&A ENTERPRISES so request,
9 the agents will, to the extent practicable, attempt to provide the employees with copies of data
10 that may be necessary or important to the continuing function of A&A ENTERPRISES CNMI
11 LLC's legitimate business. If, after inspecting the computers, it is determined that some or all of
12 this equipment is no longer necessary to retrieve and preserve the evidence, the government will
13 return it.

14 51. Computers or other devices that are seized may be retained by the government for
15 not longer than 60 days, unless that time period is extended by the court for good cause shown.
16 Drives or devices that are imaged by the government will be destroyed or returned to the owner
17 within 120 days of the execution of the warrant, or until the case and any appeal is final,
18 whichever is longer. The 120-day period may be extended by the court for good cause shown.
19 The government is not required to return any device, information, data or property that is
20 forfeitable as contraband, fruits or instrumentalities of the crime for which conviction is had, or
21 which the government is otherwise permitted by law to retain.


22 52. If upon initial review the government determines that the seized electronic
23 material contains data or information that is not within the scope the warrant, the government
24

1 will seal said data or information and will not review it further except upon further warrant or
2 order of the court.


3 **IV. CONCLUSION**

4 53. Based on the facts as set forth in this affidavit, I believe there is probable cause
5 for a search warrant authorizing the search of the premises of A&A ENTERPRISES as described
6 in Attachment A, to seek the documents and other items described in Attachment B. I have
7 shown this affidavit and the accompanying search warrant application to Assistant United States
8 Attorney Eric O'Malley, and he informs me that they are in proper form.

9
10 Respectfully submitted,

11 
12 Frederic Jonas, Special Agent
Homeland Security Investigations

13
14 Subscribed and sworn to before me on February 12, 2021.

15
16 
17 RAMONA V. MANGLONA
18 Chief Judge

ATTACHMENT A - PROPERTY TO BE SEARCHED

The property to be searched is specifically identified as the office building of A&A ENTERPRISES CNMI, LLC, located off Middle Road on Espana Street in Gualo Rai Village, Saipan, MP. The building is a one-story, green colored concrete structure believed to contain one interior room or work area and an enclosed single bathroom. The public entrance to the office is on the southern face of the building, and the building exterior has distinct white, green, and black lettering that reads "A & A ENTERPRISE, CONSTRUCTION, MANPOWER SERVICES AND GROUND MAINTENANCE PO BOX [REDACTED] SAIPAN MP 96950 TEL: [REDACTED], CELL [REDACTED]" directly above the entrance. White security bars are located over the door and windows.



ATTACHMENT B - ITEMS TO BE SEIZED

All records relating to violations of 18 U.S. Code § 1546 Fraud and Misuse of Visas, 18 U.S.C. § 1341, Mail Fraud and 18 U.S.C. § 371 Conspiracy to Defraud the United States specifically those violations occurring during or after January 1, 2018 and involving [REDACTED], Mylene CASUPANAN, Alejandro NARIO, and [REDACTED] other past or present employee or officer of A & A ENTERPRISE CNMI LLC or any other business operating under A & A ENTERPRISE CNMI LLC, including, but not limited to:

1. Records and information relating to immigration documents, specifically the I-129CW petition packets and all supporting documents or information, submitted by A & A ENTERPRISE CNMI LLC on behalf of CW-1 beneficiaries;
2. Names, addresses, telephone numbers, and any other identifying records and documents of past and present employees, business associates, and/or clients;
3. Books, records, documents, notes, correspondence, communications, receipts, photos, and any other papers relating to a scheme to defraud, including (but not limited to) papers associated with USCIS, the U.S. Postal Service, A & A ENTERPRISE CNMI LLC., or any business or employment activity of Alejandro NARIO and [REDACTED];
4. Documents, notes, correspondence, communications, and any other papers associated with the ownership, transfer, sale, disposal, or concealment of any asset that relates to a scheme to defraud, including (but not limited to) those in the name of, associated with, of interest to, or under the apparent control of Alejandro NARIO and [REDACTED];
5. Books, records, receipts, bank statements and records, money drafts, letters of credit, money orders, cashier's checks, passbooks, bank checks, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, transfer, concealment, and/or expenditure of money;
6. United States currency, securities, precious metals, jewelry, automobile titles, financial instruments including stocks and bonds in amounts indicative of the proceeds of visa and immigration document fraud, and other items of value and/or proceeds of such related activities, as well as access to locked safes and locked storage containers on the premises and curtilage;
7. Machines, instruments, equipment, and any other items that can be used to produce/create documents or falsified records;
8. Indicia of occupancy, residency, and/or ownership of the premises that is the subject of this warrant, including but not limited to utility and telephone bills, canceled envelopes, registrations, deeds and titles, receipts, and other identification documents;

9. Correspondence and relationship records including (but not limited to) letters, faxes, emails, mail, memorandums, invoices, contracts, local and long-distance phone records, address books, business cards, and photographs; and
10. Fax, typewriter ribbons, correction tapes, printer and copier toner cartridges, and hard drives of copy machines.

For any computer, electronic computing device, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, electronic computing device, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "COMPUTER" and "DEVICE"):

1. Evidence of who used, owned, or controlled the COMPUTER or DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat" or other instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control the COMPUTER or DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of the attachment to the COMPUTER or DEVICE of other storage devices or similar containers for electronic evidence;
5. Evidence of counter-forensic programs, and associated data, that are designed to eliminate data from the COMPUTER or DEVICE;
6. Evidence of the dates, times, and duration the COMPUTER or DEVICE was used;
7. Passwords, encryption codes or keys, and other access devices that may be necessary to access the COMPUTER or DEVICE;
8. Documentation and manuals that may be necessary to access the COMPUTER or DEVICE, or to conduct a forensic examination of the COMPUTER or DEVICE;
9. Records of or information about Internet Protocol addresses used or accessed by the COMPUTER or DEVICE;
10. Records of or information about the COMPUTER or DEVICE's Internet access and activity, including firewall logs, caches, browser history and cookies; "bookmarked" or saved web pages, search terms that a user entered into any Internet search engine, and records of any user-inputted web addresses; and

11. Contextual information necessary to understand the evidence described in this attachment.

As used above:

1. The terms “records” and “information” includes all forms of creation or storage, including any form of computer, electronic computing device, or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies);
2. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, tablets, mobile phones, server computers, and network hardware; and
3. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.